

## MMIC Announces New Crisis Management and Media Communications Service

When clinic administrator Carla Nelson\* realized that one of her physicians had lost a laptop containing private patient information, she panicked and her mind raced. *How would she communicate the situation to patients? What would happen if the media got hold of the story?*

### Something bad has happened. How will your clinic handle it?

During times of crisis, it's common to focus on the patient safety and legal ramifications of an issue — and ignore, procrastinate or mishandle the communication elements. After hearing from clients with dilemmas like the scenario described above, MMIC Group launched its crisis management and communications program. This new and innovative service is specifically designed to assist healthcare organizations manage a crisis, communicate with employees, patients, and the media — and minimize negative outcomes following adverse events.

MMIC Group has partnered with the Minneapolis-based Rotenberg Associates to offer these communications services to policyholders who experience a qualifying event. With a background that includes everything from medical malpractice litigation to medical device product liability, Rotenberg brings a

unique blend of media relations expertise with a keen respect for and knowledge of the law.

“We're pleased to offer our clients the service of an organization with such unique and specialized experience,” said Vice President of Sales, Marketing and Communications Julie Stafford.

“This partnership will provide a valuable service to all MMIC clients and is specifically designed to assist our clients in handling their most sensitive issues. We are proud to be one of the first in our industry to offer this valuable benefit to our policyholders.”

Rotenberg Associates, led by veteran media attorney Amy Rotenberg, along with Stacy Bettison, an experienced litigation attorney, provides complex, high-stakes communications and strategic planning for businesses, organizations and individuals.

Rotenberg and Bettison both have significant experience in healthcare and provider-related issues.



Amy Rotenberg

*(continued on back page)*

## We Heard You: MMIC Policy Documents Are Available 24/7

In recent months, our customers told us that accessing policy information can be cumbersome and time-consuming. Thanks to your feedback, we now offer online policy documents through MMIC's website, [MMICGroup.com](http://MMICGroup.com).

By accessing our site, policyholders and agents can easily view and print important documents any time of day — or night — from any computer with Internet access.

Each time a user logs in, certificates of insurance, delivery invoices and other documents are available at the click of a mouse. This new service provides a central, online location to find all of your policy information instantly and reduces the need for mailing paper documents, which can sometimes take several days to arrive.

*(continued on back page)*

\*Fictitious name.

## Health Reform: Measuring Cost and Quality

### Minnesota Introduces Provider Peer Grouping

MMIC Group is collaborating with the Minnesota Medical Association (MMA) to help educate clinic administrators and physicians about a key health reform initiative that could have broad impact on the cost and quality of care in Minnesota.

The 2008 health reform law requires the Commissioner of Health to develop a provider peer grouping system which, as described by the Minnesota Department of Health (MDH), is “a method for comparing healthcare providers based on a combination of risk-adjusted cost and quality [measures], for a provider’s total patient population, as well as for select specific health conditions.”

Once provider information is analyzed, it will be publicly reported and government and private health plans must use the peer grouping results to strengthen incentives for consumers to choose high-quality, low-cost healthcare providers. An advisory group has been working with MDH to design the peer grouping methodology.

Current plans call for reports on total care to be disseminated to healthcare providers beginning this October and to the public beginning in December. Reports on specific conditions are scheduled to be shared with providers in December and publicly reported in February 2011. Providers will have the opportunity to appeal their results based on any concerns they may have about the accuracy of the data used in the analysis.

The MMA is working closely with MDH to ensure the peer grouping methodology results include accurate and reliable information. According to Libby

Lincoln, MMIC Group Senior Vice President and General Counsel, “If that is achieved, peer grouping may become a valuable means of identifying quality improvement opportunities and assessing the success of improvement efforts.”

---

## Current plans call for reports on total care to be disseminated to healthcare providers beginning this October.

---

MMIC Group will be closely monitoring the evolution of provider peer grouping to help ensure providers have access to the resources necessary to understand the process, meet their reporting requirements and make effective use of their results.

“MMIC Health IT can help practices put the processes in place to collect and submit the data to meet reporting requirements — and MMIC Insurance risk managers can assist in using peer grouping results to implement effective quality improvement and patient safety programs,” said Lincoln.

MMA will host a series of webinars to help you learn more about provider peer grouping and what it means to your practice. For more information and to sign up, visit [www.mmaonline.net/peergrouping](http://www.mmaonline.net/peergrouping).

## We’d like to hear from you!

The *Review* newsletter is published by MMIC Group, based in Minneapolis, Minn. If you’d like to receive this newsletter electronically — or if you have comments to share with us — we’d love to receive your feedback. Please send an e-mail to: [Communications@MMICGroup.com](mailto:Communications@MMICGroup.com).

## Lawsuits: Protecting Your Practice and Your Well-being

When a patient files a lawsuit, an attorney protects your practice, but who protects you?

Working through the litigation process is one of the most difficult things a physician will ever experience on both a legal and emotional level. MMIC Group recognized these challenges and created the Physician Litigation Support Program to remove the mystery of litigation and to help prepare physicians for what they would encounter during the process.

“We surveyed our physicians and found the majority had similar comments about the malpractice litigation process,” said Vice President of Claim, Jerry Zeitlin. “Most said it was the worst experience of their lives.”

The program reduces the stress and anxiety that physicians go through during the claim and litigation process by explaining what’s happening and offering resources. It’s also MMIC’s goal to ensure physicians are able to successfully participate in their own defense and prevent the possibility of premature settlements due to the strain of the process.



Dr. Ronald Hofeldt

MMIC has partnered with Ronald Hofeldt, M.D., who has worked closely with both physician-owned insurance carriers and attorney professional liability carriers. He has more than 20 years of experience working with physician defendants and empowering them to successfully participate in the defense of their cases. A physician himself, Dr. Hofeldt works closely with the attorneys with the goal

of educating both the physician and counsel about the strategic and emotional realities of litigation.

“We had underestimated the impact a claim has on our physicians’ well-being,” Zeitlin said. “Dr. Hofeldt contacts every physician who is involved in a claim or lawsuit and is available to help during the most stressful times of litigation.”

The process begins with Dr. Hofeldt contacting a physician who is the subject of a lawsuit or claim. Typically, he speaks with the physician during the times of greatest pressure; before depositions, before trial and each night of the trial, to help relieve as much stress as possible. Specific details about the case are not discussed, and the conversations focus on the emotional impact on the physician rather than the actual litigation.

“Dr. Hofeldt doesn’t talk about the case details with our physicians,” Zeitlin said. “He talks about the emotional and physical toll the legal process is taking.

“Through this program, we’ve learned that our clients often open up more to another physician than they will to their claim representative, defense counsel or even their own family members.”

Dr. Hofeldt can provide important information to the defense team by letting them know how the physician is doing on an emotional level and how they can best prepare him or her for a deposition or trial. Most importantly, he provides coaching to help physicians maintain their practice and personal life — and manage the stress of the litigation process.

MMIC is tremendously pleased to partner with Dr. Hofeldt and offer this service to our clients during what could be the most difficult time in their careers.

For information about the Physician Litigation Support Program, contact Jerry Zeitlin at 952-838-6715 or [Jerry.Zeitlin@MMICGroup.com](mailto:Jerry.Zeitlin@MMICGroup.com).

# Administrative Proceeding Defense Coverage

## Extra Protection at No Extra Cost

Are you aware of all the coverage you have with MMIC Group? Did you know you have a policy endorsement that provides coverage for defense costs in administrative proceedings? Did you know that MMIC provides the basic limits of this coverage free of charge?

### What proceedings are covered?

Administrative Proceeding Defense Coverage (APDC) provides coverage for the defense of administrative proceedings commenced and reported to MMIC during the policy period.

It is sometimes too narrowly referred to as “Medicare Fraud and Abuse” coverage. Although many of the claims it addresses do allege fraudulent Medicare billing, the reach of its coverage is much broader. An administrative proceeding is an inquiry, investigation or other action brought against a policyholder by a managed care organization, third party payer or defined government entity:

1. that may result in suspension, revocation or limitation of medical staff or clinical privileges;
2. for alleged submission of claim(s) for reimbursement in violation of statute, regulation or contract;
3. for alleged violation of the Emergency Medical Transfer and Active Labor Act (EMTALA); or
4. for alleged violation of HIPAA regulations.

In some situations, inquiries by Recovery Audit Contractors (RACs) and actions by hospitals against medical staff or clinical privileges may also be covered.

Investigations by healthcare licensing and disciplinary boards are excluded from this definition; defense coverage for physician licensing board actions is included in the underlying professional liability policy.

### What costs are covered?

APDC pays for defense costs. These include reasonable attorney fees, additional customary costs of defense (expert witness fees, costs of transcripts, etc.) and consultant fees when the consultant is hired by the attorney.

The policy does not cover fines, repayments or other sanctions — nor does it cover expenses associated with implementing compliance plans, preparing cost reports, or responding to routine reviews by government agencies or third party payers.

### Who is covered?

APDC coverage applies to each healthcare facility, corporation, partnership, physician and surgeon listed individually in the Schedule of Insureds. Licensed employees (e.g., nurses, physician assistants) of these entities are also covered.

### How much coverage is provided?

At no additional charge, each insured person or entity receives annual coverage of \$25,000. This is an aggregate limit — the maximum available — for each person, regardless of the number of administrative actions reported during the policy year. There is an overall policy limit of \$100,000 for this basic coverage. Higher limits of coverage may be purchased.

### Who can defend me in the administrative proceeding?

To help control the quality and cost of defense, the APDC applies only if you are represented by an attorney appointed by MMIC. It does not cover any fees of any attorney not so appointed. To make sure you receive the full benefit of the APDC, contact MMIC immediately if you receive notice of an administrative proceeding, and an attorney will be retained on your behalf.

### Who should I contact for more information?

For questions about purchasing higher APDC limits, contact your underwriter, agent or broker.

For questions about specific administrative proceedings or to report an APDC claim, contact MMIC General Counsel Libby Lincoln at 800-328-5532 or 952-838-6752 or [Libby.Lincoln@MMICGroup.com](mailto:Libby.Lincoln@MMICGroup.com).

## E-mail Encryption

### *Using e-mail to send patient info?*

#### *Read this first*

Protecting patient privacy is an essential issue. With the dependence on technology, such as e-mail, to create efficiencies in workflow comes new guidelines to ensure all patient data is kept secure. The Health Insurance Portability and Accountability Act (HIPAA) specifies how your digital records containing sensitive patient information should be kept secure, ensuring that your patients' privacy is maintained.

The consequences for violating these guidelines, even unintentionally, can be costly.

While it's true that something as simple as e-mailing a document to an intended recipient could potentially violate a patient's privacy, protecting patients' data doesn't have to be a time-consuming and expensive task.

Sending e-mail in the traditional way is a little like sending a postcard through cyberspace. The information is easily available for anyone to read and for theft or tampering. Even when an e-mail makes it to your recipient's in-box, it can still be accessed by people other than the designated recipient. Something as simple as an accidental

keystroke could send an e-mail with patient data to an unknown party, increasing the severity of the security breach.

Because e-mail can provide such great workflow efficiencies, but can also be a security risk, MMIC Health IT recommends that customers implement an easy-to-use e-mail encryption service. E-mail encryption allows healthcare organizations to securely send electronic protected health information (ePHI) through e-mail.

### **A simple solution to a common scenario**

Consider this scenario: A primary care physician in your office determines that he or she would like to send a patient to another provider for further diagnosis or treatment. The physician asks the physician assistant (PA) to e-mail the patient's history, imaging reports, lab information and progress notes to the off-site healthcare provider for review. Sending an unencrypted e-mail with ePHI greatly increases your risk of exposing patient data and violating their privacy rights under HIPAA. Fortunately, using a simple e-mail encryption service will make this transmitted information safe.

### **How does encryption work?**

Encryption is the process of taking information and making it unreadable to anyone who shouldn't have access to it. Unless computer users have a special key that allows them to read the e-mail, its contents cannot be read.

One product MMIC Health IT has helped clients implement is ZixMail. When ZixMail users create an e-mail, they have the option to send it as an encrypted message. Once sent, the e-mail is routed to ZixMail, where it is encrypted, time-stamped and authenticated for proof of delivery and receipt. This "detour" to ZixMail only takes a few minutes, but adds a tremendous amount of security to your e-mail communications.





*(E-mail Encryption continued)*

HIPAA regulations require “securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.” The rules do not specify a particular technology application, so healthcare providers have a choice of tools that will best suit their needs. MMIC Health IT can help your practice assess your needs and recommend a solution that will fit easily into your current workflow.

Both sent and received e-mails are stored for 30 days and can be viewed by logging into ZixMail.

### **How do I know what information requires encryption?**

Tools like ZixMail have a built-in system that automatically detects and encrypts messages containing personally identifiable information. This option helps prevent the accidental transmission of confidential data through e-mail.

### **Who should use encrypted e-mail?**

- Physicians who send patient information
- Payers who reference any information that could be considered identifiable
- Anyone sending ePHI through e-mail

### **What are the benefits of using encrypted e-mail?**

- Compliance with HIPAA e-mail security rules
- Easy to use and administer
- Integrates with Microsoft Outlook
- Fast and easy implementation with no interruption to users
- No additional vendor management
- Low cost per user, per month

As electronic health records become more common, the risk of data exposure increases. ZixMail E-mail Encryption Services is the leader in healthcare e-mail security and e-mail encryption solutions.

For more information about encrypted e-mail or to deploy ZixMail in your practice, contact Brian Salzman at 952-838-6843 or [Brian.Salzman@MMICGroup.com](mailto:Brian.Salzman@MMICGroup.com).



## MMIC Health IT Training Opportunities

MMIC Health IT will be offering a variety of online training opportunities in the upcoming weeks. Listed below is our current schedule of events. We hope you can attend.

### **NextGen 5.6 EPM Overview**

July 23, 2010

10 a.m.

### **NextGen 5.6 EHR Overview**

July 29, 2010

10 a.m.

### **NextGen 5.6 ICS Overview**

August 16, 2010

1:30 p.m.

### **NextGen EHR System Templates**

August 26, 2010

10 a.m.

To view the training schedule, course descriptions and to register for classes, visit our training center at <https://mmic.webex.com/tc> or follow the link to the training center from the MMIC Health IT page at [MMICGroup.com](http://MMICGroup.com).

If you have any questions regarding these classes, contact the Client Support Center at [ClientSupport@MMICGroup.com](mailto:ClientSupport@MMICGroup.com) or call 952-838-6868.

## MMIC Group Named Top Workplace

MMIC Group was recently named one of the Top 100 Workplaces in the Twin Cities (Minnesota) metro area, based on an employee-based survey project from the Star Tribune newspaper. The Top Workplaces special section was published in the Star Tribune on Sunday, June 20.

The Top Workplaces program recognizes the most progressive companies in the area based on employee opinions about company leadership, career opportunities, workplace flexibility, compensation and benefits.

The analysis included responses from more than 33,000 employees at public, private and nonprofit organizations.

MMIC ranked 32 out of 45 small companies. Final rankings were based on an employee survey, which was completed earlier this year. Employees were not originally told how the survey would be used. "We didn't want the results to be skewed," said Brenda Devlin, Vice President of Human Resources. "We wanted candid, open feedback, which overall, turned out to be extremely positive."

To qualify for the Star Tribune Top Workplaces, a company must have more than 50 employees in the Twin Cities metro area. More than 1,000 companies were invited to participate.

Star Tribune Publisher Michael J. Klingensmith said, "I congratulate each of the companies in the Star Tribune Top Workplaces on their outstanding accomplishment. They have succeeded in creating a positive workplace for their employees during very challenging economic times."



7650 Edinborough Way, Suite 400  
Minneapolis, MN 55435-5978

*(Policy Documents continued from front page)*

To try out this new service, follow these steps:

1. Visit [www.MMICGroup.com](http://www.MMICGroup.com).
2. Log into your account using your usual user ID and password. (If you don't already have an online account, click the "Register" link below the log in area.)
3. Click the "My Account" button in the top navigation bar.
4. Click the "My Policies" link.
5. Click the "View" button next to the policy you'd like to access.
6. Click the "I agree" button if you agree with the terms and conditions. (You'll only need to do this once, during your initial session.)
7. To view the documents, click the yellow folder icon under the "Policy Documents" column.

If you have questions or need assistance navigating the site, contact Mike Goettl at 952-838-6804 or via e-mail: [Michael.Goettl@MMICGroup.com](mailto:Michael.Goettl@MMICGroup.com).

*(Crisis Management continued from front page)*

The firm has handled numerous high-profile matters, including medical malpractice trials and verdicts, product liability cases, infection control breaches and critical issues for both hospitals and clinics.

They regularly coordinate local, regional and national media relations — and have managed communications for product recalls, revaccination programs, state and federal regulatory investigations and HIPAA violations.

MMIC clients who need this service should contact their Risk Management or Claim Consultant.